

Structure de groupe

1 Loi de composition interne

1 Définition

Définition : loi de composition interne

Soit E un ensemble non vide.
On appelle **loi de composition interne** sur E

toute application $\star : \begin{array}{l} E \times E \longrightarrow E \\ (x, y) \longmapsto x \star y \end{array}$.

Définition : associativité, commutativité, distributivité

Une loi de composition interne \star sur un ensemble E est dite

- **associative** lorsque

$$\forall (x, y, z) \in E^3, (x \star y) \star z = x \star (y \star z)$$

(que l'on peut alors noter $x \star y \star z$.)

- **commutative** lorsque

$$\forall (x, y) \in E^2, x \star y = y \star x.$$

Si \star et \top sont deux lois de composition interne sur E , on dit que \star est **distributive** sur \top lorsque

$$\forall (x, y, z) \in E^3, x \star (y \top z) = (x \star y) \top (x \star z) \text{ et } (y \top z) \star x = (y \star x) \top (z \star x).$$

2 Élément neutre

Définition : Élément neutre

Soit \star une loi de composition interne sur E et e un élément de E .

On dit que e est **élément neutre** pour \star si pour tout $x \in E$, $x \star e = e \star x = x$.

Propriété : Unicité de l'élément neutre

S'il existe, l'élément neutre est unique.

3 Éléments symétrisable

Définition : Éléments symétrisables

Soit \star une loi de composition interne sur E , admettant un élément neutre $e \in E$.

Un élément x de E est dit **symétrisable** pour \star si on a $y \in E$ tel que $x \star y = y \star x = e$.

Définition – Propriété : Unicité du symétrique

Si \star est une loi de composition interne associative sur E , alors pour tout $x \in E$ symétrisable, l'élément y de E tel que $x \star y = y \star x = e$ est unique et appelé **symétrique** de x pour \star dans E .

Propriété

Soit \star une loi de composition interne associative sur E .

Si x et y sont symétrisables, alors

- $x \star y$ l'est aussi.
- De plus, $\text{sym}(x \star y) = \text{sym}(y) \star \text{sym}(x)$.
- $\text{sym}(x)$ l'est aussi et $\text{sym}(\text{sym}(x)) = x$.



Corollaire

- En notation additive : si x est symétrisable, alors pour tout $n \in \mathbb{N}$, nx l'est aussi et $n(-x) = -(nx)$ noté $(-n)x$.
- En notation multiplicative : si x est inversible, alors pour tout $n \in \mathbb{N}$, x^n l'est aussi et $(x^{-1})^n = (x^n)^{-1}$ noté x^{-n} .

II Structure de groupe

1 Définition

Définition : Groupe

On appelle **groupe** tout couple (G, \star) où G est un ensemble tel que

- \star est une loi de composition interne sur G
- \star est associative
- G admet un élément neutre pour \star
- Tout élément de G admet un symétrique dans G pour \star .

Si, de plus, \star est commutative, on dit que (G, \star) est un **groupe commutatif** ou **groupe abélien**.

Propriété : Exemples de groupes usuels

- $(\mathbb{C}, +)$ et $(\mathbb{C}^D, +)$ avec D ensemble non vide ont une structure de groupe additif abélien.
- (\mathbb{C}^*, \times) a une structure de groupe multiplicatif abélien.
- $(\mathcal{S}(E), \circ)$ a une structure de groupe, non commutatif en général.
Si $E = \llbracket 1, n \rrbracket$, $\mathcal{S}(E)$ est noté \mathcal{S}_n appelé **groupe symétrique** d'ordre n .

2 Groupe produit

Propriété : Groupe produit

Soit (G, \star) et (H, Δ) des groupes.
Pour tout (g, h) et (g', h') dans $G \times H$, on pose

$$(g, h) \top (g', h') = (g \star g', h \Delta h').$$

Alors $(G \times H, \top)$ a une structure de groupe.
Si, de plus, les lois \star et Δ sont commutatives, alors \top l'est.

3 Sous-groupes

a Définition

Définition : Sous-groupe

Soit (G, \star) groupe.
On dit que H est un **sous-groupe** de (G, \star) si $H \subset G$ et $(H, \star|_{H^2})$ est un groupe.
On note $H < G$.

Propriété : Sous-groupes triviaux

Soit (G, \star) groupe.
 G et $\{e_G\}$ sont des sous-groupes de (G, \star) appelés **sous-groupes triviaux**.

b Caractérisation

Propriétés

- Soit H un sous-groupe de (G, \star) .
- (H, \star) possède le même élément neutre que (G, \star) .
 - Si $x \in H$, alors x a même inverse dans (H, \star) et dans (G, \star) .

Propriété

Soit (G, \star) un groupe. Les propositions suivantes sont équivalentes :

- H est un sous-groupe de (G, \star)

$$\left\{ \begin{array}{l} H \subset G \\ H \neq \emptyset \quad (e_G \in H) \\ H \text{ est stable par } \star : \forall x, y \in H, x \star y \in H \\ H \text{ et par inverse} : \forall x \in H, \text{sym}(x) \in H \end{array} \right.$$
- $$\left\{ \begin{array}{l} H \subset G \\ H \neq \emptyset \quad (e_G \in H) \\ \forall x, y \in H, x \star \text{sym}(y) \in H \end{array} \right.$$

Propriété : Exemples de groupes usuels

- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{R}^D, +)$ ont une structure de groupe additif abélien.
- (\mathbb{Q}^*, \times) , (\mathbb{Q}_+^*, \times) , (\mathbb{R}^*, \times) , (\mathbb{R}_+^*, \times) , (\mathbb{U}, \times) , (\mathbb{U}_n, \times) pour $n \in \mathbb{N}^*$ ont une structure de groupe multiplicatif abélien.

c Intersection, réunion, produit

Propriété : Intersection de sous-groupes
Soit G un groupe et $(H_i)_{i \in I}$ une famille de sous-groupes de (G, \star) . Alors $\bigcap_{i \in I} H_i$ est un sous-groupe de (G, \star) .

Propriété : Réunion de sous-groupes
Soit (G, \star) un groupe, H, K sont des sous-groupes de (G, \star) , alors
 $H \cup K$ sous-groupe de $(G, \star) \iff H \subset K$ ou $K \subset H$.

d Sous-groupes de $(\mathbb{Z}, +)$

Notation
Pour tout $a \in \mathbb{Z}$, on note $a\mathbb{Z} = \{ak, k \in \mathbb{Z}\}$.

Théorème : Division euclidienne dans \mathbb{Z}
Soient $a \in \mathbb{Z}, b \in \mathbb{N}^*$. Il existe un unique couple $(q, r) \in \mathbb{Z}^2$ tel que
$$\begin{cases} a = bq + r \\ 0 \leq r < b \end{cases}$$

 q est le **quotient** et r est le **reste** de la division euclidienne de a par b .

Propriété : Sous-groupes de $(\mathbb{Z}, +)$
Les sous-groupes G de $(\mathbb{Z}, +)$ sont exactement les $a\mathbb{Z}$ pour $a \in \mathbb{N}$.
De plus, si $G \neq \{0\}$, $a = \min(G \cap \mathbb{N}^*)$.

4 Morphismes de groupes

a Définition

Définition
Soient (G, \star) et (G', \bullet) deux groupes.
 $f : (G, \star) \rightarrow (G', \bullet)$ est un **morphisme de groupes** si et seulement si
$$\forall (x, y) \in G^2, f(x \star y) = f(x) \bullet f(y)$$

Définition
Lorsque $(G, \star) = (G', \bullet)$, on parle d'**endomorphisme** de groupes.
Lorsque f est bijective, on parle d'**isomorphisme**.
Lorsqu'il existe un isomorphisme entre G et G' , on dit que G et G' sont **isomorphes**.
Lorsque f est bijective et $G = G'$, on parle d'**automorphismes**.

5 Propriétés

Propriété
Si $f : (G, \star) \rightarrow (G', \bullet)$ est un morphisme de groupes, alors $f(e_G) = e_{G'}$ et pour tout $x \in G$, $f(\text{sym}(x)) = \text{sym}(f(x))$.

Propriété : Image directe ou réciproque d'un sous-groupe par un morphisme de groupe
Soit $f : (G, \star) \rightarrow (G', \bullet)$ un morphisme de groupes.
(i) Si H est un sous-groupe de (G, \star) , alors $f(H)$ est un sous-groupe de (G', \bullet)
(ii) Si H' est un sous-groupe de (G', \bullet) , $f^{-1}(H')$ est un sous-groupe de (G, \star) .

Propriété
Si $f : (G, \star) \rightarrow (G', \bullet)$ et $g : (G', \bullet) \rightarrow (G'', \Delta)$ sont des morphismes de groupes, alors $g \circ f$ en est encore un.

Propriété
Soit $f : (G, \star) \rightarrow (G', \bullet)$ un isomorphisme de groupes.
Alors f^{-1} est un isomorphisme du groupe (G', \bullet) sur le groupe (G, \star) .

Propriété
On note $\text{Aut}(G)$ l'ensemble des automorphismes du groupe (G, \star) .
Alors $(\text{Aut}(G), \circ)$ a une structure de groupe.

a Noyau et image

Définition : Image et noyau d'un morphisme de groupes

Soit $f : (G, \star) \rightarrow (G', \bullet)$ un morphisme de groupes.

On appelle **noyau** de f :

$$\text{Ker } f = f^{-1}(\{e_{G'}\}) = \{x \in G \mid f(x) = e_{G'}\}.$$

Ainsi, $x \in \text{Ker } f \iff f(x) = e_{G'}$.

On appelle **image** de f :

$$\text{Im } f = f(G) = \{f(x), x \in G\}.$$

Ainsi, $y \in \text{Im } f \iff \exists x \in G, y = f(x)$.

Propriété

Soit $f : (G, \star) \rightarrow (G', \bullet)$ un morphisme de groupe.

- f est injectif si et seulement si $\text{Ker } f = \{e_G\}$.
- f est surjectif si et seulement si $\text{Im } f = G'$.

Propriété

Soit $f : (G, \star) \rightarrow (G', \bullet)$ un morphisme de groupes.

Alors $\text{Ker } f$ est un sous-groupe de G et $\text{Im } f$ est un sous-groupe de G' .

Propriété

(\mathfrak{S}_n, \circ) est un groupe d'ordre (ie de cardinal) $n!$, non abélien dès que $n \geq 3$.

b Ordre d'une permutation

Définition

L'ordre d'une permutation σ est le plus petit $k \in \mathbb{N}^*$ tel que $\sigma^k = \text{id}$.

Propriété

L'ordre d'une permutation de \mathfrak{S}_n est bien défini et vaut au plus l'ordre $n!$ de ce groupe.

c Orbites et support

Définition : Orbites

Soit $\sigma \in \mathfrak{S}_n$. La relation binaire définie sur $\llbracket 1, n \rrbracket$ par

$$x \sim y \iff \exists k \in \mathbb{Z}, y = \sigma^k(x)$$

est une relation d'équivalence dont les classes d'équivalence sont les **orbites** de σ .

Si $x \in \llbracket 1, n \rrbracket$,

$$\mathcal{O}(x) = \{\sigma^k(x), k \in \mathbb{Z}\}.$$

Propriété

Soit $\sigma \in \mathfrak{S}_n, x \in \llbracket 1, n \rrbracket$. Alors il existe $\ell \in \mathbb{N}$ tel que $\mathcal{O}(x) = \{x, \sigma(x), \dots, \sigma^{\ell-1}(x)\}$ (deux à deux distincts).

Définition : Support

Si $\sigma \in \mathfrak{S}_n$, son **support** est l'ensemble des éléments de $\llbracket 1, n \rrbracket$ qui **ne sont pas** invariants par σ .

Propriétés

- (i) $\text{Supp}(\sigma)$ est stable par σ .
- (ii) Deux permutations à supports disjoints commutent.

III Groupe symétrique

1 Permutations

a Définition

Définition : Permutation, groupe symétrique

Si E est un ensemble, on appelle **permutation** de E toute bijection de E dans E . On note $\mathfrak{S}(E)$ leur ensemble.

Si $E = \llbracket 1, n \rrbracket = \llbracket 1, n \rrbracket$ où $n \in \mathbb{N}^*$, on note \mathfrak{S}_n appelé **groupe symétrique d'ordre n (ou de degré n)** cet ensemble.

Si $\sigma \in \mathfrak{S}_n$, on note

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n) \end{pmatrix}.$$

d Transpositions, cycles

On suppose ici $n \geq 2$.

Définition : Transposition

Une **transposition** τ est une permutation qui échange deux éléments i et j de $\llbracket 1, n \rrbracket$, et laisse les autres invariants ie dont le support est $\{i, j\}$.
 On la note $\tau = (i\ j)$ ou parfois $\tau_{i,j}$.
 $\tau_{i,j}(i) = j, \tau_{i,j}(j) = i$ et si $k \notin \{i, j\}, \tau_{i,j}(k) = k$.

Définition : Cycle

Soit $p \in \mathbb{N}$ tel que $2 \leq p \leq n$.
 On appelle **p -cycle** une permutation c de \mathfrak{S}_n qui permute circulairement p éléments i_1, i_2, \dots, i_p de $\llbracket 1, n \rrbracket$ et laisse les autres invariants ie dont le support est $\{i_1, \dots, i_p\}$ et telle que
 $c(i_1) = i_2 ; c(i_2) = i_3 ; \dots ; c(i_{p-1}) = i_p ; c(i_p) = i_1$
 p est la **longueur** du cycle c . On note $c = (i_1\ i_2\ \dots\ i_p)$.

Propriété

(i) $i_1\ i_2\ \dots\ i_p = (i_1\ i_p)(i_1\ i_{p-1})\dots(i_1\ i_2)$
 $= (i_1\ i_2)(i_2\ i_3)\dots(i_{p-1}\ i_p)$.

(ii) Un p -cycle est d'ordre p .

Théorème

Toute permutation se décompose en produit (composée) de cycles à supports disjoints. La décomposition est unique à l'ordre des facteurs près.

Corollaire

Toute permutation se décompose en produit de transpositions.

2 Morphisme de signature et sous-groupe alterné

On fixe $n \in \mathbb{N}^*$.

a Signature d'une permutation

Définition : Inversions, signature

Soit $\sigma \in \mathfrak{S}_n$. On appelle **inversion** par σ tout couple (i, j) tel que $i < j$ et $\sigma(i) > \sigma(j)$.
 On note $I(\sigma)$ le nombre d'inversions par σ .
 On appelle **signature** de σ le nombre $\varepsilon(\sigma) = (-1)^{I(\sigma)} \in \{-1, 1\}$.
 Une permutation σ est dite **paire** lorsque $I(\sigma)$ est pair et donc $\varepsilon(\sigma) = 1$. Elle est dite **impaire** dans le cas contraire.

 **Méthode : Détermination pratique du nombre d'inversions**

Pour chaque nombre de la deuxième ligne (image), on compte le nombre de nombres plus petits situés à sa droite. Et on fait la somme.

Propriété

Toute transposition est impaire.

Lemme : Expression de la signature

Soit $\sigma \in \mathfrak{S}_n$.

$$\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i} = \prod_{\{i,j\} \in \mathcal{D}} \frac{\sigma(j) - \sigma(i)}{j - i}$$

où $\mathcal{D} = \{\{i, j\} \mid 1 \leq i \leq n \text{ et } 1 \leq j \leq n \text{ et } i \neq j\}$ désigne l'ensemble des paires d'entiers distincts compris entre 1 et n .

Théorème

Soit $n \geq 2$. L'application

$$\varepsilon : \begin{cases} (\mathfrak{S}_n, \circ) & \longrightarrow & (\{-1, 1\}, \times) = (\mathbb{U}_2, \times) \\ \sigma & \longmapsto & \varepsilon(\sigma) \end{cases}$$

est un morphisme de groupe, ie si $\sigma, \sigma' \in \mathfrak{S}_n$, $\varepsilon(\sigma\sigma') = \varepsilon(\sigma)\varepsilon(\sigma')$.



Propriétés

- (i) Un produit de deux permutations de même parité est pair, un produit de deux permutations de parités différentes est impair.
- (ii) Si $\sigma \in \mathfrak{S}_n$ se décompose en produit de N transpositions, $\varepsilon(\sigma) = (-1)^N$.
En particulier, cette décomposition n'est pas unique mais la parité du nombre de termes est toujours celle de la permutation.
- (iii) ε est le seul morphisme de groupes de \mathfrak{S}_n dans $\{-1, 1\}$ tel que $\varepsilon(\tau) = -1$ pour toute transposition τ . (C'est en fait aussi le seul morphisme de groupe surjectif.)
- (iv) Si c est un p -cycle, $\varepsilon(c) = (-1)^{p-1}$.
- (v) Si $\sigma \in \mathfrak{S}_n$, $\varepsilon(\sigma^{-1}) = \varepsilon(\sigma)$.

b

Groupe alterné (HP)

Définition : Groupe alterné

Le sous-groupe $\mathfrak{A}_n = \text{Ker}(\varepsilon)$ des permutations paires de \mathfrak{S}_n est appelé **groupe alterné d'ordre n (ou de degré n)**.

Propriété

Pour tout $n \geq 2$, $|\mathfrak{A}_n| = \frac{n!}{2}$.